CLAIM LISTING

This listing of claims will replace all prior versions, and listings of claims in the application:

In the Claims

1. (Currently amended) ~~An encryption key stored in a~~ PLD comprising:

a plurality of programmable logic resources;

a configuration control circuit coupled to the plurality of programmable logic resources;

a key memory coupled to the configuration control circuit and having stored therein a plurality of key bits for defining an encryption algorithm, ~~,~~ and at least one bit for indicating whether more keys will follow.

2. (Currently amended) The PLD ~~encryption key~~ of Claim 1 wherein the at least one bit for indicating whether more keys will follow comprises:

two bits for indicating whether the key is first, middle, last, or only of a set of keys.

3. (Currently amended) The PLD ~~encryption key~~ of Claim 1 wherein the plurality of key bits comprises 56 bits.

4. (Currently amended) The PLD ~~encryption key~~ of Claim 1 wherein the encryption algorithm comprises the DES algorithm.

5. (Currently amended) The PLD ~~encryption key~~ of Claim 1 wherein the at least one bit for indicating whether more keys will follow is one bit.

6. (Currently amended) The PLD ~~encryption key~~ of Claim 1 wherein the ~~a~~least one bit for indicating whether more keys will follow specifies the number of additional keys that will follow.

7. (Currently amended) The PLD ~~encryption key~~ of Claim 1 wherein the at least one bit for indicating whether more keys will follow specifies whether the key is a first key.

8. (Currently amended) The PLD ~~encryption key~~ of Claim 1 wherein the at least one bit for indicating whether more keys will follow specifies whether the key is a last key.

9. (New) A method for configuring a programmable logic device (PLD), comprising:

storing in the PLD a plurality of decryption keys and in association with each key at least one respective bit that indicates whether the key is a last of the plurality of keys to be used in decrypting an input value;

receiving a configuration bitstream at the PLD, wherein the configuration bitstream includes control data and words of configuration data and at least the configuration data is encrypted;

decrypting each encrypted word of the configuration bitstream in the PLD using each of the plurality of decryption keys and completing decryption of the word in response to the associated bit of a decryption key indicating the decryption key is the last decryption key, whereby a decrypted configuration bitstream is generated; and

storing configuration data from the decrypted configuration bitstream in configuration memory of the PLD.

10. (New) The method of claim 9, further comprising disabling readback of configuration data from the PLD after storing the configuration data in configuration memory.

11. (New) The method of claim 10, further comprising disabling partial reconfiguration of the PLD in response to decryption of the configuration bitstream.

12. (New) The method of claim 9, wherein the at least one bit respectively associated with each decryption key includes two bits that indicate whether the key is a first key, a middle key, or the last key to be used in the decrypting step.

13. (New) The method of claim 9 wherein each decryption key bits includes 56 bits.

14. (New) The method of claim 9 wherein the decrypting step includes performing DES decryption.

15. (New) The method of claim 9, wherein the step of storing the plurality of decryption keys includes inputting a boundary scan instruction to the PLD.

16. (New) The method of claim 9, wherein the at least one bit respectively associated with each decryption key includes a plurality of bits, and each plurality indicates one of an address of a next decryption key to be used in decrypting a word and the last decryption key.

17. (New) An apparatus for configuring a programmable logic device (PLD), comprising:

means for storing in the PLD a plurality of decryption keys and in association with each key at least one respective bit that indicates whether the key is a last of the plurality of keys to be used in decrypting an input value;

means for receiving a configuration bitstream at the PLD, wherein the configuration bitstream includes control data and

words of configuration data and at least the configuration data is encrypted;

means for decrypting each encrypted word of the configuration bitstream in the PLD using each of the plurality of decryption keys and completing decryption of the word in response to the associated bit of a decryption key indicating the decryption key is the last decryption key, whereby a decrypted configuration bitstream is generated; and

means for storing configuration data from the decrypted configuration bitstream in configuration memory of the PLD.

18. (New) A programmable logic device (PLD), comprising:

a configuration memory;

programmable logic circuitry coupled to the configuration memory;

a key management circuit adapted for storage of a plurality of keys and in association with each key at least one respective bit that indicates whether the key is a last of the plurality of keys to be used in decrypting an input value;

a configuration circuit coupled to the configuration memory and to the plurality of storage elements, the configuration circuit adapted to receive an encrypted input configuration bitstream and configure the configuration memory with a decrypted version of the input configuration bitstream; and

a decryptor coupled to the configuration circuit and to the plurality of storage elements, the decryptor configured to decrypt, responsive to the configuration circuit, each encrypted word of configuration bitstream using each of the plurality of decryption keys and completing decryption of the word in response to the at least one associated bit of a decryption key indicating the decryption key is the last decryption key, whereby the decrypted version of the input configuration bitstream is generated.

19. (New) The PLD of claim 18, wherein the at least one bit respectively associated with each decryption key includes two bits that indicate whether the key is a first key, a middle key, or the last key to be used by the decryptor.

20. (New) The PLD of claim 18 wherein each decryption key bits includes 56 bits.

21. (New) The PLD of claim 18 wherein the decryptor is adapted to perform DES decryption.

22. (New) The PLD of claim 18, further comprising a boundary scan interface coupled to the key management circuit, the boundary scan interface adapted to write the decryption keys to storage of the key management circuit responsive to input boundary scan instructions.

23. (New) The PLD of claim 18, wherein the at least one bit respectively associated with each decryption key includes a plurality of bits, and each plurality indicates one of an address of a next decryption key to be used in decrypting a word and the last decryption key, and the decryptor being adapted to read a next decryption key responsive to an address associated with a current decryption key.

24. (New) The PLD of claim 18, wherein the configuration circuit is further adapted to disable partial reconfiguration of the PLD responsive to completion of configuration with the decrypted version of the configuration bitstream.

25. (New) The PLD of claim 24, wherein the configuration circuit is further adapted to disable readback of configuration data from the PLD responsive to completion of configuration with the decrypted version of the configuration bitstream.